Double Random Phase Encryption Based Orthogonal Encoding Technique for Color Images

In-Ho Lee and Myungjin Cho*

*Department of Electrical, Electronic, and Control Engineering, Hankyong National University,
Ansung 456-749, Korea*

(Received March 11, 2014 : revised March 20, 2014 : accepted March 27, 2014)

In this paper, we propose a simple Double random phase encryption (DRPE) -based orthogonal encoding technique for color image encryption. In the proposed orthogonal encoding technique, a color image is decomposed into red, green, and blue components before encryption, and the three components are independently encrypted with DRPE using the same key in order to decrease the complexity of encryption and decryption. Then, the encrypted data are encoded with a Hadamard matrix that has the orthogonal property. The purpose of the proposed orthogonal encoding technique is to improve the security of DRPE using the same key at the cost of a little complexity. The proposed orthogonal encoder consists of simple linear operations, so that it is easy to implement. We also provide the simulation results in order to show the effects of the proposed orthogonal encoding technique.

Keywords : Optical encryption, Double-random-phase encryption, Orthogonal encoding

OCIS codes : (060.4785) Optical security and encryption; (200.4560) Optical data processing

I. INTRODUCTION

In data transmission, encryption techniques are necessarily required in order to prevent unauthorized access. Thus, encryption techniques have been widely studied [1-18]. In particular, optical encryption techniques with an advantage in terms of the encryption speed have been well researched [5-16]. Double random phase encryption (DRPE), which is the most widely used optical encryption technique, has been proposed [5]. It can be implemented easily and its speed of encryption is faster than that of non-optical encryption methods. DRPE employs two independent random phase masks to encrypt the primary image. Although such an optical encryption technique improves the security of the transmission information, color information cannot be handled in decryption since the primary image is illuminated with monochromatic light [19].

DRPE-based encryption techniques for a color image have been presented [19, 20]. The color image encryption using fractional Fourier transforms [19] and the color image encryption by wavelength multiplexing based on lensless Fresnel transform holograms [20] have been proposed. In

these techniques, the color image is separated into red, green, and blue components, and they are independently encrypted. Also, these techniques use many keys for both encryption and decryption. Though the data security can improve with an increase in the number of keys or the length of keys, the encryption and decryption system can become more complicated as the amount of key information rises.

In this paper, we propose a simple DRPE-based orthogonal encoding technique for color image encryption. In the proposed technique, a color image is segregated into red, green, and blue components before encryption and each of the components is independently encrypted, analogous to the previous encryption techniques. However, we employ DRPE using the same key in encrypting three components in order to reduce the complexity of encryption and decryption, unlike the previous cases. In addition, we adopt a Hadamard matrix [21] with orthogonal property in order to encode the encrypted data in each of red, green, and blue channels. The orthogonal encoding scheme is able to enhance the security of DRPE using the same key for three components at the expense of a little complexity. Furthermore, the

*Corresponding author: mjcho@hknu.ac.kr

Color versions of one or more of the figures in this paper are available online.

orthogonal encoder is easy to implement because it consists of simple linear operations. Therefore, the proposed DRPE-based orthogonal encoding technique can be a low-complexity and effective encryption technique for color images.

The paper is organized as follows. First we briefly present the DRPE in Section II. Then, the orthogonal encoding technique using DRPE is described in Section III. To show the effects of DRPE-based orthogonal encoding technique, simulation results are provided in Section IV. Finally, we conclude the paper with a summary in Section V.

II. DOUBLE RANDOM PHASE ENCRYPTION

Optical encryption has many advantages such as the parallel processing of optical systems, the fast processing time, and the data handling in various domains. One of the optical encryption methods, double random phase encryption (DRPE), uses two sets of random phase information. Let us consider the encryption of a one-dimensional signal for simplicity. Figure 1(a) shows the optical schematic setup

(a)

(b)

FIG. 1. Optical schematic setup of double-random-phase encryption technique for (a) encryption and (b) decryption.

of DRPE for encryption. Let $s(x)$ be the primary data. Then, for encryption, we use two uniformly distributed random noises over $[0, 1]$ which are $n_s(x)$ in the spatial domain and $n_f(\mu)$ in the spatial frequency domain. First, the random phase noise, $\exp[i2\pi n_s(x)]$ multiplies the primary data, $s(x)$. Then, this data passes through lens 1 which means a Fourier transform of $s(x)\exp[i2\pi n_s(x)]$. To obtain the convolution result between $s(x)\exp[i2\pi n_s(x)]$ and $h(x)$ where the Fourier transform of $h(x)$ is $\mathcal{F}\{h(x)\} = \exp[i2\pi n_f(\mu)]$, their Fourier transforms are multiplied by each other. Finally, the inverse Fourier transform of this data can be recorded through lens 2. That is, the encrypted data by DRPE, $s_e(x)$ is a complex-valued function as the following: [13]

$$s_e(x) = \mathcal{F}^{-1} \left[\mathcal{F} \left\{ s(x) \exp[i2\pi n_s(x)] \right\} \exp[i2\pi n_f(\mu)] \right] \quad (1)$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ mean Fourier transform and inverse Fourier transform, respectively. By the characteristics of complex-valued function, encrypted data has amplitude and phase, i.e., $s_e(x) = |s_e(x)|\exp[i\phi_e(x)]$.

Figure 1(b) illustrates the optical schematic setup of DRPE for decryption. To decrypt the primary data, encrypted data as shown in Eq. (1) is multiplied by the complex-conjugate of the Fourier transform of $h(x)$ as the following: [13]

$$s_d(x) = \left| \mathcal{F}^{-1} \left\{ \mathcal{F} \left[s_e(x) \right] \exp[-i2\pi n_f(\mu)] \right\} \right| \quad (2)$$

III. DRPE-BASED ORTHOGONAL ENCODING TECHNIQUE

Figures 2(a) and (b) show the orthogonal encoding procedure using DRPE for encryption and decryption, respectively. As shown in Fig. 2(a), the primary color image, $p(x)$, is decomposed into red, green, and blue components, $s^R(x)$, $s^G(x)$, and $s^B(x)$, before DRPE. Then, the DRPE of the three components is independently performed, but with the same key information, as depicted in Fig. 2(a). Thus, after DRPE, three encrypted data, $s_e^R(x)$, $s_e^G(x)$, and $s_e^B(x)$, are obtained in red, green, and blue channels, respectively. Then, three encoded data, $c^R(x)$, $c^G(x)$, and $c^B(x)$, are obtained by encoding the encrypted data of red, green, and blue channels, respectively, with the orthogonal code. Note that the encrypted and encoded data are complex-valued.

To acquire the primary color image, first the three encoded data are independently decoded with the orthogonal property used in the encoder, and then the three decoded data, $\tilde{s}_e^R(x)$, $\tilde{s}_e^G(x)$, and $\tilde{s}_e^B(x)$, are decrypted as depicted in Fig. 2(b). Finally the three decrypted data, $s_d^R(x)$, $s_d^G(x)$, and $s_d^B(x)$, are composed to obtain the color image.

For orthogonal encoding and decoding, we use the Hadamard matrix of order 2, denoted by $\mathbf{H}_2$, with the orthogonal

without decoding are still encrypted ones even though the decryption is done with the perfect key information. On the other hand, when the key information of DRPE is known, the decrypted images with decoding as shown in Figs. 7(a)~(d) perfectly match with the primary images in Figs. 4(a)~(d).

Table 1 shows mean square error (MSE) results for the images as shown in Figs. 4~6, where it is assumed that the pixel intensity (integer value) range of each image is from 0 to 255. The values of three different columns in

Table 1 are MSE results between primary and encoded images, between encrypted and encoded images, and between primary and incorrectly decrypted images for red channel, green channel, and blue channel, respectively. From MSE results, it is illustrated that compared images are clearly different from each other.

FIG. 4. Primary color image with (a) full color channels, (b) red channel, (c) green channel, and (d) blue channel.

FIG. 5. Simulation results of DRPE-based orthogonal encoding for a color image. (a) encrypted image of red channel, (b) encrypted image of green channel, (c) encrypted image of blue channel, (d) encoded image of red channel, (e) encoded image of green channel, and (f) encoded image of blue channel.

FIG. 6. Simulation results of decryption of DRPE-based orthogonal encoding for a color image without decoding. (a) decrypted image of red channel, (b) decrypted image of green channel, (c) decrypted image of blue channel, and (d) decrypted full color image.

FIG. 7. Simulation results of decryption of DRPE-based orthogonal encoding for a color image with decoding. (a) decrypted image of red channel, (b) decrypted image of green channel, (c) decrypted image of blue channel, and (d) decrypted full color image.

TABLE 1. MSE results for the images as shown in Figs. 4-6

	MSE between primary and encoded images	MSE between encrypted and encoded images	MSE between primary and incorrectly decrypted images
Red channel	5422.5	537.7	4592.6
Green channel	4805.0	521.9	4042.9
Blue channel	3666.1	513.0	3095.1

V. CONCLUSION

In this paper, we have proposed the DRPE-based orthogonal encoding technique for encryption of color images. To encrypt each of red, green, and blue components of a color image, the proposed orthogonal encoding technique employs DRPE with the same key and the orthogonal encoding scheme that uses the simple linear operations with a little complexity. Also, for decryption, we provide the orthogonal decoding scheme that has the same structure as the encoding scheme. The simulation results show that the proposed orthogonal encoding technique provides the powerful encryption effects in the absence of the orthogonal decoding although the key information of DRPE is perfectly known. Hence, the proposed orthogonal encoding technique can be used as a low-complexity and effective encryption technique for color images.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2013-067321) and this research was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2057549).

REFERENCES

1. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Inf. Theory* **39**, 1639-1646 (1993).
2. C. Rackoff and D. Simon, "Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Proc. Crypto' 91*, 433-444 (1991).
3. S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal on Selected Areas in Communication* **7**, 467-473 (1989).
4. H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Proc. Crypto' 87*, 341-349 (1987).
5. P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767-769 (1995).
6. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," *Appl. Opt.* **38**, 7288-7293 (1999).
7. T. Nomura and B. Javidi, "Optical encryption system with a binary key code," *Appl. Opt.* **39**, 4783-4787 (2000).
8. M. Singh, A. Kumar, and K. Singh, "Secure optical system that uses fully phase-based encryption and lithium niobate crystal as phase contrast filter for decryption," *Opt. Laser Technol.* **40**, 619-624 (2008).
9. Z. Liu, S. Li, M. Yang, W. Liu, and S. Liu, "Image encryption based on the random rotation operation in the fractional Fourier transform domains," *Opt. Lasers Eng.* **50**, 1352-1358 (2012).
10. M. Joshi, C. Shakher, and K. Singh, "Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys," *Opt. Commun.* **283**, 2496-2505 (2010).
11. Z. Liu, S. L. Xu, C. Lin, J. Dai, and S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains," *Opt. Lasers Eng.* **49**, 542-546 (2011).
12. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," *Appl. Opt.* **46**, 6641-6647 (2007).
13. E. Perez-Cabre, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.* **36**, 22-24 (2011).
14. T. Sarkadi and P. Koppa, "Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys," *Appl. Opt.* **51**, 745-750 (2012).
15. T. Ujvári, P. Koppa, M. Lovasz, P. Varhegyi, S. Sajti, E. Lorincz, and P. Richter, "A secure data storage system based on phase-encoded thin polarization holograms," *J. Opt. A: Pure Appl. Opt.* **6**, 401-411 (2004).
16. P. Koppa, "Phase-to-amplitude data page conversion for holographic storage and optical encryption," *Appl. Opt.* **46**, 3561-3571 (2007).
17. Z. Liu, M. Yang, W. Liu, S. Li, M. Gong, W. Liu, and S. Liu, "Image encryption algorithm based on the random local phase encoding in gyrator transform domains," *Opt. Commun.* **285**, 3921-3925 (2012).
18. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.* **38**, 3198-3201 (2013).
19. M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," *Opt. Commun.* **279**, 35-42 (2007).
20. L. F. Chen and D. M. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Opt. Express* **14**, 8552-8560 (2006).
21. J. J. Sylvester, "Thoughts on orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers," *Phil. Mag.* **34**, 461-475 (1867).